Configure NTP Authentication Failure on ISE 3.4 Due to HEX Prefix Handling

Contents

Issue

Cisco Identity Services Engine (ISE) 3.4.0.608 Patch 1 fails to synchronize with NTP servers when using authenticated NTP with SHA1 keys that are 40 characters in length. The NTP authentication key commands are accepted on CLI without error, but NTP synchronization does not occur when authentication is enabled. Without authentication, NTP synchronization works correctly. Other network devices, including Cisco switches, successfully authenticate with the same NTP server using identical key ID and key values.

During troubleshooting, packet capture analysis revealed that ISE sends authenticated NTP requests with proper Key ID and MAC/authenticator fields, however, the server replies contain a Key ID of all zeros and no MAC/authenticator, causing ISE to reject the authentication. Debug output on Cisco switches acting as NTP servers displayed "SHA1-Match: 0" indicating authentication failure.

Environment

- Cisco Identity Services Engine (ISE) Version 3.4.0.608 with Patch 1
- NTP Authentication using SHA1 algorithm
- NTP Authentication keys of 40 characters in length
- Cisco Catalyst 9500 Switches (C9500-24Y4C) running Version 17.12.04
- NTP Server Appliances with Authenticated NTP Configuration

Resolution

This issue is caused by Cisco bug ID: CSCwq79772, which affects how ISE handles long NTP authentication keys when the HEX prefix is required. This bug was fixed in ISE 3.4 Patch 8 and ISE 3.5 Patch 3.

Understanding the Root Cause

When configuring NTP authentication keys on Cisco devices, keys that are 20 characters or longer are automatically treated as hexadecimal strings rather than plain text. This requires ISE to use the "HEX:" prefix when configuring the key. However, due to the bug, ISE only accepts 36 characters of a 40-character key because of the additional "HEX:" prefix handling, resulting in authentication failure.

Immediate Workaround Options

Until ISE software can be upgraded to a version containing the fix, use one of these workarounds:

Option 1: Use a 36-Character SHA1 Key

Configure both the NTP server and ISE with a 36-character SHA1 key instead of the 40-character key.

On ISE:

```
ntp authentication-key 1 sha1 plain HEX:1d3f35b762ab7c21e5f1265dc9762fe421fa
```

On the NTP server (Cisco switch example):

```
ntp authentication-key 1 sha1 1d3f35b762ab7c21e5f1265dc9762fe421fa
ntp authenticate
ntp trusted-key 1
```

Option 2: Use MD5 Authentication

Switch from SHA1 to MD5 authentication, which does not exhibit the same length limitation.

On ISE:

```
ntp authentication-key 1 md5 plain [MD5-key-value]
ntp server [NTP-server-IP] key 1
```

On the NTP server:

```
ntp authentication-key 1 md5 [MD5-key-value]
ntp authenticate
ntp trusted-key 1
```

Verification Steps

After implementing either workaround, verify NTP synchronization:

On ISE:

```
show ntp
show clock
```

On the switch (if using switch as NTP server):

```
show ntp associations
show ntp status
```

Look for successful synchronization indicators and verify the authentication is working by confirming NTP synchronization fails when authentication is disabled on one side but enabled on the other.

Permanent Resolution

Upgrade ISE to one of the these versions that contains the fix for Cisco bug ID: CSCwq79772:

- ISE 3.4 Patch 8 (when available)
- ISE 3.5 Patch 3 or later

After upgrading, the original 40-character SHA1 key configuration works correctly with the HEX prefix.

Cause

This issue is caused by Cisco bug ID: CSCwq79772, in ISE versions prior to 3.4 Patch 8 and 3.5 Patch 3. When NTP authentication keys are 20 characters or longer, Cisco devices treat these as hexadecimal strings, requiring the "HEX:" prefix in the configuration. Due to this bug, ISE incorrectly handles the key length calculation when the HEX prefix is used, accepting only 36 characters of a 40 character key. This results in a key mismatch between ISE and the NTP server, causing authentication failure during NTP synchronization attempts.

Related Content

- Cisco Bug CSCwq79772
- Cisco Wireless Controller Command Reference - NTP Authentication
- Cisco Technical Support & Downloads